5. Интернет-портал Минкомсвязь России [Электронный ресурс] / Минкомсвязь России. — Режим доступа: http://www.minsvyaz.ru. — Дата доступа: 30.10.2017.

УДК 343.98+004.7

В. В. Молоков
начальник кафедры информационно-правовых дисциплин
и специальной техники
Сибирского юридического института МВД России,
кандидат технических наук, доцент

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Одной из актуальных проблем масштабной информатизации государственной, экономической, социальной сфер общества и частной жизни человека является угроза противоправных деструктивных действий, исходящая со стороны пространства сети Интернет. Это прежде всего преступления, связанные с мошенничеством, кибератаками, схемами нелегального бесконтактного сбыта наркотиков, экономическими преступлениями и т. п. К сожалению, все эти факты являются обратной стороной технологического прогресса. Это не может не вызывать озабоченности государства и, как следствие, усиления мер противодействия преступлениям, совершаемым посредством сети Интернет [1]. Важную роль в борьбе с такого рода преступлениями занимают правоохранительные органы и органы государственной безопасности.

Выделим факторы, способствующие совершению преступлений с использованием сети Интернет:

Огромная популярность Всемирной паутины и интернет-сервисов.

Наличие средств анонимизации пользователей в сети. Использование анонимных прокси-серверов, VPN-туннелей, децентрализованных сетей типа Tor.

Широкое применение методов криптографии.

Популярность криптовалют и технологий блокчейн.

Перечисленный арсенал интернет-технологий при их грамотном использовании значительно затрудняет, а то и делает невозможным процесс успешного раскрытия и расследования преступлений, совершаемых посредством сети Интернет. Мнимая уверенность в безнаказанности неявно совершаемых деяний провоцирует новые преступления и способствует вовлечению в этот процесс молодых лиц.

Рассмотрим основные методы и мероприятия, составляющие основу системы противодействия преступлениям, совершаемым посредством сети Интернет:

1. Выявление и профилактика.

2. Оперативно-техническое противодействие.

3. Совершенствование проведения оперативно-розыскных мероприятий в сети Интернет.

4. Государственный и ведомственный контроль за интернет-компаниями.

5. Международное сотрудничество.

Выявление и профилактика преступлений — одни из основных задач, стоящих перед органами внутренних дел. Преступления, совершаемые с использованием сети Интернет, обладают высокой латентностью. Часть преступлений становятся известными дефакто после наступления последствий, как, например, мошенничество или кража денег с электронных счетов. Другие — преступления типа незаконного оборота наркотиков — могут выявляться на стадии их совершения. Для этого используются средства мониторинга информационного пространства Всемирной паутины и методы интернет-разведки. Профилактика преступлений в основном ориентирована на повышение грамотности пользователей интернет-пространства, их самостоятельное противодействие угрозам персональных и личных данных. Многие преступления в сфере мошенничества могут предотвратить сами пользователи, если будут соблюдать элементарные меры безопасности при работе с интернет-сервисами и другими электронными средствами.

Техническое противодействие могло бы быть наиболее эффективным средством предотвращения или раскрытия преступлений, совершаемых с использованием сети Интернет. Однако оно требует серьезных финансовых вложений, высокой квалификации специалистов и координации усилий интернет-компаний. В настоящий

момент основным средством технического противодействия является механизм блокировки провайдерами ресурсов сети Интернет, содержащих противоправный контент. Регулятором этого процесса является Роскомнадзор, который ведет «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено». Работа в этом направлении проводится системно, и поставленные перед службой задачи решаются успешно. Тем не менее смена хостинга сайта не является для злоумышленников большой проблемой.

Гораздо более интересными являются методы оперативно-технического противодействия. Речь идет об эффективном использовании системы технических средств для обеспечения функций оперативно-розыскных мероприятий. Внедрение систем на основе DPI (технологий глубокого анализа трафика) могло бы способствовать решению задачи деанонимизации пользователей, совершающих противоправные деяния и скрывающих свое пребывание в сети Интернет. Неразрывно с техническим оснащением оперативных подразделений должна решаться задача повышения уровня квалификации сотрудников в сфере специальных технических знаний, необходимых для раскрытия и расследования преступлений, совершаемых посредством сети Интернет. Оперативные сотрудники в состоянии самостоятельно решать некоторые технические задачи по установлению значимой информации в интересах раскрытия такого рода преступлений. Повышение квалификации сотрудников органов внутренних дел в этом направлении в настоящий момент проводится регулярно.

Следующее направление совершенствования оперативно-розыскных мероприятий связано с получением информации в открытых источниках [2]. Современный человек оставляет о себе в сети Интернет огромное количество информации: социальные сети, интернет-мессенджеры, сервисы медиа-контента и т. п. Использование методов интернет-разведки и эффективных приемов поиска информации в сети Интернет может дать дополнительную информацию, имеющую значение для успешного раскрытия или расследования преступлений различных видов [3].

В качестве примера государственного регулирования деятельности интернет-компаний можно привести Федеральный закон от 06.07.2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». Положения статьи 15 Федерального закона обязывают организаторов распространения информации в сети Интернет хранить как факты передачи различных типов сообщений, так и их содержимое. Однако есть проблемы, связанные с действием норм отечественного законодательства на зарубежные интернет-компании, осуществляющие свою деятельность на территории Российской Федерации, как, например, мессенджеры Telegram, Signal и т. п.

И наконец, следует затронуть тему международного сотрудничества в вопросах противодействия преступлениям, совершаемым с использованием сети Интернет. Преодоление противодействия раскрытию и расследованию преступлений, которые осуществляют преступные элементы и группы, возможны только усилиями всего мирового сообщества. В этом случае инструменты сокрытия информации абонентов могут перестать быть таковыми, и вопросы установления лица, совершающего преступление под маской анонима, не будут проблемой. Однако мы можем констатировать, что в основном большая часть уголовных преступлений, связанных с использованием сети Интернет, раскрывается и расследуется в рамках одной страны.

В заключение следует сказать, что накоплен большой опыт по раскрытию и расследованию преступлений, совершаемых с использованием сети Интернет, создана база оперативно-технического противодействия, решаются задачи оперативно-розыскных мероприятий во Всемирной паутине, ведется подготовка оперативных сотрудников в области специальных технических знаний, что не может не вызывать оптимизма. Остается надеяться на улучшение международного сотрудничества.

Список основных источников

1. Молоков, В. В. Методы противодействия использованию сети интернет террористическими организациями / В. В. Молоков, П. В. Галу-

шин // Противодействие идеологии экстремизма и терроризма в молодежной среде (отечественный и зарубежный опыт) : материалы межрегион. науч.-практ. конф. с междунар. участием / ред.-изд. группа: О. В. Локота (рук.), С. А. Воронцов (зам. рук.). — Ростов-н/Д, 2017. — С. 198–202.

2. Галушин, П. В. Выявление латентных связей в социальных сетях в целях противодействия незаконному обороту наркотиков / П. В. Галушин // Вестник Сибирского юридического института МВД России. — 2017. — № 1 (26). — С. 54–58.

3. Охота, Г. Н. Оперативно-розыскное противодействие незаконному обороту наркотиков с использованием ресурсов сети «Интернет» / Г. Н. Охота, А. А. Помелов // Современность в творчестве начинающего исследователя : сборник материалов Всероссийской научно-практической конференции молодых ученых / Восточно-Сибирский институт МВД России. — Иркутск, 2017. — С. 164–168.

УДК 004.056+347.157

М. Ю. Пакляченко

преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга Воронежского института МВД России, кандидат технических наук

М. А. Ледовская

преподаватель кафедры информационной безопасности Краснодарского университета МВД России

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ И ПУТИ ИХ РЕШЕНИЯ

Ведущие ученые в области информационной безопасности [1–3] в числе наиболее актуальных проблем выделяют защиту детей от информации, причиняющей вред их здоровью и развитию.

Актуальность защиты от подобного рода информации обусловлена особой уязвимостью детей, которые в условиях стремительного развития информационных технологий в наибольшей степени подвержены негативному информационному воздействию. Информация, распространяемая в телекоммуникационных сетях, может оказывать на детей психотравмирующее и растлевающее